UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,341	09/12/2003	Bernd Meyer	P2001,0154	8043

7590 01/10/2007

LERNER AND GREENBERG, P.A.
POST OFFICE BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
LASHLEY, LAUREL L	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/661,341	MEYER ET AL.	
	Examiner	Art Unit	
	Laurel Lashley	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. ______.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/16/2006 has been entered.

2. It is noted that while Applicant has submitted claim amendments, arguments responsive to the previous Office action (Advisory Action, dated: 10/13/2006) were not submitted therefore the rejection is maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1 – 6, 13 – 16 and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Hopkins in US Patent 5,757,918 (hereinafter US '918).

4. As it relates to claim 1, US '918 teaches:

A method for authenticating a data set between a proving unit and a verifying unit, which comprises the steps of (see US '918: Abstract):

a) communicating the data set from one of the proving and verifying units to a respective other of the proving and verifying units such that the data set is in an unencrypted form to both the proving and verifying units after completing step a) (see US '918: column 3, lines 13 – 14);

b) generating at least one data element in the verifying unit (see US '918: column 3, line 26);

c) using the verifying unit to encrypt the data element in a first cryptographic encryption method using a public key of the proving unit resulting in at least one encrypted data element, and the public key is known to the verifying unit (see US '918: column 4, lines 39 – 40);

d) communicating the encrypted data element from the verifying unit to the proving unit (see US '918: column 4, lines 42 – 44);

e) using the proving unit to decrypt the encrypted data element in a first decryption method, assigned to the first cryptographic encryption method, using a private key known only to the proving unit (see US '918: column 3, lines 27 – 28);

f) using the proving unit to calculate, from the data set to be authenticated, in a second cryptographic method, an authenticator dependent on the data element (see US '918: column 3, lines 25 –30);

g) communicating the authenticator from the proving unit to the verifying unit (see US 918: column 3, lines 25 – 30);

h) using the verifying unit to check the authenticator with an aid of an authentication checking algorithm, assigned to the second cryptographic method using the data element and the data set (see US '918: column 3, lines 31 – 33); and

i) accepting the data set as communicated by the proving unit to the verifying unit is dependent on a result of the check performed in step h) (see US '918: column 3, lines 34 – 37).

For claim 2, US '918 teaches:

The method according to claim 1, which further comprises during the step a), using the proving unit to communicate the data set in unencrypted form to the verifying unit (see US '918: column 3, lines 13 – 14).

For claim 3, US '918 teaches:

The method according to claim 1, which further comprises using the verifying unit to generate

the data set as a random element and subsequently, in the step a), communicating the data set to the proving unit (see US '918: column 3, lines 13 – 14).

For claim 4, US '918 teaches:

The method according to claim 1, which further comprises during the step h):

forming the authentication checking algorithm to be substantially identical to the second cryptographic method for authenticator generation;

applying the authentication checking algorithm by the verifying unit to the data element and the data set for forming a reference authenticator; and

comparing the reference authenticator with the authenticator (see US '918: column 3, lines 31 – 33, 54 – 60 and column 4, lines 39 – 40).

As for claim 5, US '918 teaches:

The method according to claim 1, which further comprises during the step h):

forming the authentication checking algorithm with a decryption method corresponding to the second cryptographic method for generating the authenticator for an associated encryption method;

applying the authentication checking algorithm by the verifying unit to the authenticator by decryption for forming a reference data element and a reference data set; and

comparing the reference data element and the reference data set with the data element and the data set (see US '918: column 3, lines 54 –60 and column 4, lines 39 – 40).

As for claim 6, US '918 teaches:

The method according to claim 1, which further comprises:

repeating steps b), c), d) and e) for generating at least one further data element before performing the step f); and

using the proving unit to encrypt the data set to be authenticated in step f) in a manner dependent on the data element and the further data element to form the authenticator (see US '918 column 2, lines 46 – 48 and column 4, lines 42 – 44).

As for claim 13, US '918 discloses:

The method according to claim 1, which further comprises performing the following steps before performing step b):

using the proving unit to communicate the public key with a certificate of a trust center;

using the verifying unit to check a validity of the public key of the proving unit using a certification method; and

using the verifying unit to continue the communication with the proving unit in a manner dependent on a result of the check (see US '918: column 2, line 56 – column 3, lines 1 – 5).

For claim 14, US '918 teaches:

The method according to claim 1, which further comprises:

forming the proving unit as an integrated circuit on a smart card; and

forming the verifying unit as a smart card terminal (see US '918: column 2, lines 27 – 29).

As for claim 15, US '918 teaches:

The method according to claim 1, which further comprises forming the proving unit as an integrated circuit in an identification/authentication token which is fixedly connected to a non-localized object (see US '918: column 4, lines 58 – 66).

As for claim 16 and 21, US '918 teaches:

The methods according to claims 14 and 15 respectively, which further comprises performing the communication between the proving unit and the verifying unit contactlessly (see US '918: column 2, lines 32 –36).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 7 – 12 and 17 – 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins (US Patent 5,757,918) in view of Miyaji et al. in US Patent 5,272,755.

6. Regarding claims 7 and 8, Hopkins discloses:

carrying out the first cryptographic encryption method and the first decryption method (see US '918: column 3, lines 31 – 33, 54 – 60 and column 4, lines 39 – 40)

but does not show

using discrete exponentiation in a semigroup *or* using an algorithm based on elliptical curves (as in claims 7 and 8 respectively).

Miyaji et al. however does disclose using discrete exponentiation in a semigroup (see US '755: column 12, line 28) *and* using an algorithm based on elliptical curves (see US '755: column 15, lines 7 –22).

For claims 7 and 8, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the first cryptographic encryption method of Hopkins to use discrete exponentiation in a semigroup as in Miyaji et al. The motivation for doing so would have been to reduce costs and the technical implementation outlay in the authentication of data while providing a high degree of security.

As for claims 9 and 17, Hopkins discloses:

performing the first cryptographic encryption method using the verifying unit,

using the verifying unit to calculate an element,

using the verifying unit to calculate from the public key, *and*

using the verifying unit to encrypt the at least one data element,

but does not teach

generat[ing] a number $t \in T$, where T is a subrange of integers;

or

calculat[ing] element $h^{f(t)} \in H$, where $f : T \rightarrow T'$ is a mapping into a subrange T' of the integers, which is not necessarily different from T, H represents a multiplicatively written semigroup generated by element h, with a discrete exponentiation of a base h as a one-way function in the semigroup H;

or

[calculating] $k_{pub} = h^{f(d)} \in H$, element $\pi(k_{pub}{}^{f(t)}) \in G$, where $\pi : H \rightarrow G$ specifies a mapping of the semigroup H into a group G, $d \equiv k_{priv} \in T$ is the private key which is accessible only to the proving unit, and a mapping $t \rightarrow h^{f(t)} \rightarrow \pi(k^{f(t)})$ from the subrange of the integers T to the group G represents a one-way function; and

or

[encrypting] z, by a combination with respect to the encrypted data element, $z' = z \circ \pi(k_{pub}{}^{f(t)}) \in G$.

Miyaji et al. however does show

generat[ing] a number $t \in T$, where T is a subrange of integers;

using the verifying unit to calculate element $h^{f(t)} \in H$, where $f : T \rightarrow T'$ is a mapping into a subrange T' of the integers, which is not necessarily different from T, H represents a multiplicatively written semigroup generated by element h, with a discrete exponentiation of a base h as a one-way function in the semigroup H;

and

calculat[ing] $k_{pub} = h^{f(d)} \epsilon H$, element $\pi (k_{pub}{}^{f(t)}) \epsilon G$, where $\pi : H \rightarrow G$ specifies a mapping of the semigroup H into a group G, $d \equiv k_{priv} \epsilon T$ is the private key which is accessible only to the proving unit, and a mapping $t \rightarrow h^{f(t)} \rightarrow \pi (k^{f(t)})$ from the subrange of the integers T to the group G represents a one-way function; and

encrypt[ing] the at least one data element, z, by a combination with respect to the encrypted data element, $z' = z \circ \pi (k_{pub}{}^{f(t)}) \epsilon G$ (see US '755: column 1, lines 40 – 50, column 11, lines 68 – column 12, lines 1 – 9: where it is obvious that if the GF (2^n) computations are employed then instance arithmetic calculations are relied upon).

For claims 9 and 17, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the first cryptographic encryption method of Hopkins to incorporate the discrete exponentiation in a semigroup as in Miyaji et al. The motivation for doing so would have to reduce costs and the technical implementation outlay in the authentication of data while providing a high degree of security.

Regarding claims 10 and 18, Miyaji et al. in view of Hopkins teaches as a method according to claim 9, which further comprises during the step d), in addition to the encrypted data element, using the verifying unit to communicate the element $h^{f(t)} \epsilon H$ to the proving unit (see US '918: column 3, lines 26 – 27).

As for claims 11 and 19, US '918 teaches:

performing the first cryptographic decryption method,

using the proving unit to calculate the element and inverse element (see US '918: column 3, lines 25 – 30) *and*

using the proving unit to decrypt the encrypted data element (see US '918: column 3, lines 27 – 28)

but does not disclose:

calculat[ing] $k_{pub}^{f(t)} \epsilon H$ using function f, the element $h^{f(t)} \epsilon H$ and the private key d known only to the proving unit; *or*

calculat[ing] an inverse element $\pi' (k_{pub}^{f(t)}) \epsilon G$ with respect to element $\pi (k_{pub}^{f(t)}) \epsilon G$; and decrypt[ing] the encrypted data element by a combination of the encrypted data element with inverse element: $z = z' \circ \pi' (k_{pub}^{f(t)})$, where the first cryptographic decryption method is based on the same mappings f, π and the same combination $\circ$ as the first cryptographic encryption method.

Miyaji et al. however does show

calculat[ing] $k_{pub}^{f(t)} \epsilon H$ using function f, the element $h^{f(t)} \epsilon H$ and the private key d known only to the proving unit; *or*

calculat[ing] an inverse element $\pi' (k_{pub}^{f(t)}) \epsilon G$ with respect to element $\pi (k_{pub}^{f(t)}) \epsilon G$; and decrypt[ing] the encrypted data element by a combination of the encrypted data element with inverse element: $z = z' \circ \pi' (k_{pub}^{f(t)})$, where the first cryptographic decryption method is based on the same mappings f, π and the same combination $\circ$ as the first cryptographic encryption method (see US '755: column 1, lines 40 – 50, column 11, lines 68 – column 12, lines 1 – 9).

For claims 11 and 19, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the first cryptographic decryption method of Hopkins to incorporate the inverse calculation of the discrete exponentiation as in Miyaji et al. The motivation for doing so would have been to reduce costs and the technical implementation outlay in the authentication of data while providing a high degree of security.

Regarding claims 12 and 20, US '918 discloses:

performing the second cryptographic method, using the proving unit to calculate, using the proving unit to transform the data set (see US '918: column 3, lines 25 – 30)

but does not teach

calculat[ing] from at least one unencrypted data element z, an element $g_2 = \pi_1(z) \in G_1$ and an element $g_2 = \pi_2(z) \in G_2$, where G_{-1} and G_2 represent groups where G_1 subset G_2 and $\pi_1 : G \rightarrow G_1$ and $\pi_2 : G \rightarrow G_2$ represent functions which map elements of the group G onto the groups G_1 or G_2;

transform[ing] the data set to be authenticated m, to form an element $g' = (g_1 * m)$ with a group combination * in G_1; and

calculat[ing] D, by $D = inj(g') \cdot g_2$ with the group combination $\cdot$ in G_2, where the mapping $inj : G_1 \rightarrow G_2$ maps elements from G_1 injectively into G_2.

Miyaji et al. however does show

calculat[ing] from the at least one unencrypted data element z, an element $g_2 = \pi_1(z) \in G_1$ and an element $g_2 = \pi_2(z) \in G_2$, where G_{-1} and G_2 represent groups where G_1 subset G_2 and $\pi_1 : G \rightarrow G_1$ and $\pi_2 : G \rightarrow G_2$ represent functions which map elements of the group G onto the groups G_1 or G_2;

transform[ing] the data set to be authenticated m, to form an element $g' = (g_1 * m)$ with a group combination * in G_1; and

calculat[ing] D, by $D = inj(g') \cdot g_2$ with the group combination $\cdot$ in G_2, where the mapping $inj : G_1 \rightarrow G_2$ maps elements from G_1 injectively into G_2 (see US '755: column 1, lines 40 – 50, column 11, lines 68 – column 12, lines 1 – 9).

For claims 12 and 20, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the second cryptographic method of Hopkins to incorporate the injective mapping of elements as in Miyaji et al. The motivation for doing so would have been to reduce costs and the technical implementation outlay in the authentication of data while providing a high degree of security.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132
05 January 2007
LLL

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100